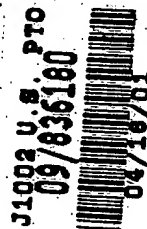


日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。 #3

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出 願 年 月 日
Date of Application:

2000年12月11日

出 願 番 号
Application Number:

特願2000-375406

出 願 人
Applicant (s):

三菱電機株式会社

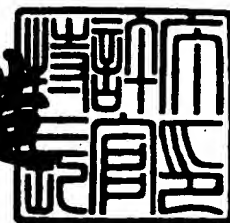
BEST AVAILABLE COPY

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 1月 5日

特 許 庁 長 官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3110238

【書類名】 特許願

【整理番号】 527084JP01

【提出日】 平成12年12月11日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/00

【発明者】

【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社
社内

【氏名】 ▲高▼本 元晴

【発明者】

【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社
社内

【氏名】 島田 豊治

【特許出願人】

【識別番号】 000006013

【氏名又は名称】 三菱電機株式会社

【代理人】

【識別番号】 100064746

【弁理士】

【氏名又は名称】 深見 久郎

【選任した代理人】

【識別番号】 100085132

【弁理士】

【氏名又は名称】 森田 俊雄

【選任した代理人】

【識別番号】 100091409

【弁理士】

【氏名又は名称】 伊藤 英彦

【選任した代理人】

【識別番号】 100096781

【弁理士】

【氏名又は名称】 堀井 豊

【選任した代理人】

【識別番号】 100096792

【弁理士】

【氏名又は名称】 森下 八郎

【手数料の表示】

【予納台帳番号】 008693

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 ログイン認証装置、およびログイン認証方法

【特許請求の範囲】

【請求項 1】 イン트라ネットを介して端末およびウェブサーバと接続可能なログイン認証装置であって、

ユーザの識別子と、前記識別子のユーザが閲覧可能なウェブサーバ内のウェブページのアドレスと、前記識別子のユーザがその内容について変更可能なウェブページのアドレスとを記憶する記憶手段と、

前記端末から受信した識別子を前記記憶手段により記憶した識別子と照合し、前記端末から受信した識別子に対して、前記ウェブページの閲覧可否および変更可否を判断する認証手段とを含む、ログイン認証装置。

【請求項 2】 前記記憶手段は、前記ユーザの識別子と、前記閲覧可能なウェブページおよび前記変更可能なウェブページとを対応付けてテーブルに記憶する、請求項 1 に記載のログイン認証装置。

【請求項 3】 前記ログイン認証装置はさらに、
前記識別子の属性ごとに前記各ウェブページへのアクセス回数をアクセス情報として集計する集計手段を含み、

前記記憶手段は、前記アクセス情報を記憶する、請求項 1 または請求項 2 に記載のログイン認証装置。

【請求項 4】 イン트라ネットを介して端末およびウェブサーバと接続可能なログイン認証装置を用いたログイン認証方法であって、

ユーザの識別子と、前記識別子のユーザが閲覧可能なウェブサーバ内のウェブページのアドレスと、前記識別子のユーザがその内容について変更可能なウェブページのアドレスとを記憶するステップと、

前記端末から受信した識別子を前記記憶するステップで記憶した識別子と照合し、前記端末から受信した識別子に対して、前記ウェブページの閲覧可否および変更可否を判断するステップとを含む、ログイン認証方法。

【請求項 5】 前記記憶するステップは、前記ユーザの識別子と、前記閲覧可能なウェブページおよび前記変更可能なウェブページとを対応付けてテーブル

に記憶する、請求項 4 に記載のログイン認証方法。

【請求項 6】 前記識別子の属性ごとに前記各ウェブページへのアクセス回数をアクセス情報として集計するステップをさらに含み、

前記記憶するステップは、前記アクセス情報を記憶する、請求項 4 または請求項 5 に記載のログイン認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、ログイン認証装置、およびログイン認証方法に関し、さらに詳しくは、イントラネットを介して端末およびウェブサーバと接続可能なログイン認証装置、およびログイン認証方法に関する。

【0002】

【従来の技術】

近年情報技術の発達に伴い、企業内でイントラネットの構築がさかんに行なわれている。

【0003】

イントラネットを構築する企業の中でも、規模の大きい企業では、たとえば、本社を中心として、各支社や各工場ごとに、または各部署ごとにウェブサーバを設置している。

【0004】

【発明が解決しようとする課題】

これらの複数のウェブサーバは、セキュリティ確保のために、ユーザ ID やパスワードの入力をユーザに要求する認証管理をそれぞれ独立して行なっている。そのため、ユーザが複数のウェブサーバにアクセスを繰返して業務を行なう場合に、各ウェブサーバにアクセスするたびに、各ウェブサーバごとのユーザ ID とパスワードの入力が必要となり、ユーザにとって非常に煩雑な作業となっていた。

【0005】

また、各ウェブサーバは複数のウェブページを有しているため、セキュリティ

補償のためウェブページ単位でも認証管理を行なう方が好ましい。しかしながらウェブサーバごとだけでなく、ウェブサーバ内のウェブページ全てについて認証管理を行なうことはユーザの操作を極めて煩雑とし、さらに、認証管理費用も増大する。よってウェブページごとの認証管理は省略せざるを得ず、ウェブサーバ単位で認証管理を行なっていた。

【 0 0 0 6 】

ネットワーク上での認証方法については、特開平 1 0 - 1 7 7 5 5 2 号公報および特開平 1 0 - 1 0 5 5 1 6 号公報にて提案されているが、ウェブサーバ内のウェブページ単位までセキュリティ補償を行なうものではなく、また、設定環境もイントラネットとは異なる環境である。

【 0 0 0 7 】

この発明の目的は、イントラネット内のウェブサーバにおいて、ウェブページ単位でセキュリティを補償し、かつユーザにとって操作が簡単であるログイン認証装置および認証方法を提供することである。

【 0 0 0 8 】

【課題を解決するための手段】

この発明に係るログイン認証装置は、イントラネットを介して端末およびウェブサーバと接続可能なログイン認証装置であって、ユーザの識別子と、上記識別子のユーザが閲覧可能なウェブサーバ内のウェブページのアドレスと、識別子のユーザがその内容について変更可能なウェブページのアドレスとを記憶する記憶手段と、上記端末から受信した識別子を上記記憶手段により記憶した識別子と照合し、上記端末から受信した識別子に対して、上記ウェブページの閲覧可否および変更可否を判断する認証手段とを含む。

【 0 0 0 9 】

好ましくはさらに、上記記憶手段は、上記ユーザの識別子と、上記閲覧可能なウェブページまたは上記変更可能なウェブページとを対応付けてテーブルに記憶する。

【 0 0 1 0 】

これにより、ウェブサーバ単位ではなくウェブページ単位でセキュリティの確

保が可能となり、かつ、ユーザはウェブページごとにユーザIDとパスワードを入力するといった煩雑な操作を行なう必要がなくなる。

【0011】

さらに好ましくは、上記ログイン認証装置は、上記識別子の属性ごとに上記各ウェブページへのアクセス回数をアクセス情報として集計する集計手段を含み、上記記憶手段は、上記アクセス情報を記憶する。

【0012】

これにより、ユーザに属性ごとのウェブページ利用回数を容易に確認することが可能となり、今後のウェブページの運用方針を決定するのに有効な判断要素となる。

【0013】

この発明に係るログイン認証方法は、イントラネットを介して端末およびウェブサーバと接続可能なログイン認証装置を用いたログイン認証方法であって、ユーザの識別子と、上記識別子のユーザが閲覧可能なウェブサーバ内のウェブページのアドレスと、上記識別子のユーザがその内容について変更可能なウェブページのアドレスとを記憶するステップと、上記端末から受信した識別子を上記記憶するステップで記憶した識別子と照合し、上記端末から受信した識別子に対して、上記ウェブページの閲覧可否および変更可否を判断するステップとを含む。

【0014】

好ましくはさらに、上記記憶するステップは、上記ユーザの識別子と、上記閲覧可能なウェブページまたは上記変更可能なウェブページとを対応付けてテーブルに記憶する。

【0015】

これにより、ウェブサーバ単位ではなくウェブページ単位でセキュリティの確保が可能となり、しかもユーザはウェブページごとにユーザIDとパスワードを入力するといった煩雑な操作を行なう必要がなくなる。

【0016】

さらに好ましくは、上記識別子の属性ごとに上記各ウェブページへのアクセス回数をアクセス情報として集計するステップをさらに含み、上記記憶するステッ

ブは、上記アクセス情報を記憶する。

【0017】

これにより、ユーザの属性ごとのウェブページ利用回数を容易に確認することが可能となり、今後のウェブページの運用方針を決定するのに有効な判断要素となる。

【0018】

【発明の実施の形態】

以下、発明の実施の形態を図面を参照して詳しく説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0019】

図1はこの発明の実施の形態であるログイン認証システムの全体構成を示すブロック図である。

【0020】

図1を参照して、企業内の各工場または各営業所である拠点イ内に設置されたログイン認証装置300は、ファイアウォール200、イントラネット100を介して所外端末10～Nと接続されている。

【0021】

また、拠点イ内においてログイン認証装置300は、所内端末1～nと、プロキシウェブサーバ400とに接続されている。プロキシウェブサーバ400はウェブページA1～A3を有するウェブサーバAと、ウェブページB1～B3を有するウェブサーバBと、ウェブページC1～C3を有するウェブサーバCとに接続可能である。なお、図1においてはプロキシウェブサーバ400に接続可能なウェブサーバは3つとしているが、プロキシウェブサーバ400が、3つ以上のウェブサーバと接続することも当然可能である。

【0022】

ログイン認証装置300は、認証部301と、マスタファイル302と、集計部303とを含む。

【0023】

マスタファイル302は、各ウェブサーバA～Cの各ウェブページごとに接続

可能なユーザの識別子であるユーザIDやパスワードを表1に示すような認証テーブルとして記憶している。

【0024】

【表1】

ユーザID	パスワード	許可コンテンツ									人事・職制情報		
		サーバA			サーバB			サーバC			工場コード	部コード	課コード
		A1	A2	A3	B1	B2	B3	C1	C2	C3			
A001	XX010		○	●							KUMA	AXX	100
	利用回数		126	59									
A002	AAb1	○									KUMA	BXX	200
	利用回数	15											
B003	CO26		●		●	○					ITAMI	YXX	300
	利用回数		50		48	10							
B004	ax9935x3										FUKU	SXX	400
	利用回数							●		300			

【0025】

なお、表1中の「●」印は、該当するウェブページの内容を閲覧することができただけでなく、その内容を変更または更新することができることを示している

。また、「○」印は、該当するウェブページの内容を閲覧することはできるが、その内容を変更または更新することはできないことを示している。たとえば、表 1 中のユーザ ID が A 0 0 1 のユーザはウェブサーバ A 中のウェブページ A 2 についてはその内容の閲覧はできるが、内容の変更または更新はできず、ウェブページ A 3 については、その内容の閲覧だけでなく、変更または更新も可能なことを表わしている。また、それ以外のウェブページについては閲覧も変更または更新もできないことを表わしている。

【 0 0 2 6 】

なお、認証テーブルには、人事・職制情報として各ユーザ ID の所属する工場コードや部コード、課コードが登録されている。

【 0 0 2 7 】

また、各ユーザがアクセスしたウェブページの利用回数についても表 1 に示すように記録される。

【 0 0 2 8 】

ログイン認証装置 3 0 0 中の認証部 3 0 1 は、各ウェブサーバ A ～ C 内のウェブページへの接続を希望するユーザが使用する所外端末 1 0 ～ N および所内端末 1 ～ n から送信されたユーザ ID およびパスワードと、マスタファイル 3 0 2 中に記憶してある認証テーブル中のユーザ ID およびパスワードを照合し、さらに、ユーザが接続を希望するウェブページの閲覧可否、更新可否を判断する。

【 0 0 2 9 】

また、ログイン認証装置 3 0 0 中の集計部 3 0 3 は各ユーザがウェブページにアクセスした回数をカウントし、定期的にカウントした結果を職制ごとに集計する機能を有する。

【 0 0 3 0 】

図 2 は、図 1 に示したログイン認証システムにおいて、ユーザが所外端末 1 0 を用いてウェブページにアクセスする場合のログイン認証システムの動作を示すフローチャート図である。

【 0 0 3 1 】

図 2 を参照して、ユーザが所外端末 1 0 を用いて、拠点イ内のウェブサーバ A

内のウェブページA 2 をアクセスしたい場合、ユーザは所外端末1 0 にユーザIDおよびパスワードおよびアクセスしたいウェブページA 2 のアドレスをキーボードやマウス等の入力部（図示せず）により入力後、拠点イ内に設置されたログイン認証装置3 0 0 に向け送信する（ステップS 1）。

【0 0 3 2】

送信されたユーザIDおよびパスワードおよびウェブページA 2 のアドレスはイントラネット1 0 0 を介してファイアウォール2 0 0 で受信される（ステップS 1 1）。

【0 0 3 3】

ファイアウォール2 0 0 は所外端末1 0 ～N から拠点イ内のウェブサーバA ～C への不正なアクセスを遮断するために設けられるシステムである。ファイアウォール2 0 0 内には拠点イ内のウェブサーバA ～C にアクセス可能なユーザIDとパスワードが予め登録されており、ファイアウォール2 0 0 内に予め登録されているユーザIDおよびパスワードと、所外端末1 0 から送信されたユーザIDおよびパスワードの照合が行なわれる（ステップS 1 2）。

【0 0 3 4】

ステップS 1 2 での照合の結果、ファイアウォール2 0 0 内に予め登録されたユーザIDおよびパスワードと、所外端末1 0 から送信されたユーザIDおよびパスワードが一致しない場合は、ファイアウォール2 0 0 は所外端末1 0 へ閲覧不可の通知を送信し（ステップS 1 3）、イントラネット1 0 0 を介して所外端末1 0 で受信される（ステップS 2）。

【0 0 3 5】

一方、ファイアウォール2 0 0 での照合の結果、ファイアウォール2 0 0 内に予め登録されたユーザIDおよびパスワードと、所外端末1 0 から送信されたユーザIDおよびパスワードが一致した場合は、ファイアウォール2 0 0 はユーザIDとパスワードと所外端末1 0 で入力されたウェブページA 2 のアドレスを拠点イ内のログイン認証装置3 0 0 へ送信する（ステップS 1 2）。

【0 0 3 6】

ログイン認証装置3 0 0 は、ファイアウォール2 0 0 からユーザIDとパスワ

ードとウェブページA 2 のアドレスを受信後（ステップS 2 1）、受信したユーザIDおよびパスワードが認証テーブル上のユーザIDおよびパスワードと一致しているか否かを認証部3 0 1で確認し、さらに受信したウェブページA 2 へのアクセス希望に対して、ユーザがアクセス可能か否かを認証部3 0 1で確認する（ステップS 2 2）。なお確認は表1に示したマスタファイル3 0 2に記憶している認証テーブルを用いて行われる。

【0 0 3 7】

ここで、ユーザIDおよびパスワードが認証テーブル上のユーザIDおよびパスワードと一致していない場合は拠点イ内のウェブサーバへのアクセスはできないので閲覧不可の通知を送信する（ステップS 2 3）。送信された閲覧不可通知はファイアウォール2 0 0を介して（ステップS 1 4）、所外端末1 0で受信される（ステップS 3）。

【0 0 3 8】

また、ユーザIDおよびパスワードが認証テーブル上のユーザIDおよびパスワードと一致していても、認証テーブル上でウェブページA 2の閲覧が許可されていないければ、ウェブページA 2を閲覧することはできない。

【0 0 3 9】

たとえば、所外端末1 0からウェブページA 2の閲覧を希望したユーザのユーザIDがA 0 0 1であった場合は、表1に示した認証テーブル上にて「○」印が記録されているので閲覧は可能である。しかし、ユーザIDがA 0 0 2のユーザは認証テーブル上のウェブページA 2欄に印が記録されていないことから、ユーザIDがA 0 0 2のユーザは拠点イ内のウェブサーバには接続可能であるが、ウェブページA 2は閲覧ができないということになる。よって、この場合においても、ユーザIDがA 0 0 2のユーザが利用している所外端末1 0に対して、閲覧不可通知を送信する（ステップS 2 3）。

【0 0 4 0】

ユーザIDがA 0 0 1のユーザのように、ウェブページの閲覧が可能と認証部3 0 1で判断された場合は、ウェブページA 2のアドレスがプロキシウェブサーバ4 0 0に送信される（ステップS 2 4）。送信されたウェブページA 2のアド

レスはプロキシウェブサーバ400で受信され（ステップS31）、プロキシウェブサーバ400はユーザが希望するウェブページを閲覧可能な状態とする（ステップS32）。

【0041】

一方、ユーザがウェブページA2内の内容について変更や更新を行なう場合もある。この場合も認証部301でユーザがウェブページA2に対して変更または更新が可能か否かを判断する。たとえば、ユーザIDがA001のユーザは表1の認証テーブルではウェブページA2欄に「○」印が記録されており、ウェブページA2について閲覧は可能であるが変更または更新はできないということになる。よって、ユーザIDがA001のユーザが所外端末10のキーボードやマウス等の入力部（図示せず）を用いてウェブページA2の内容を変更または更新しようとしたときに、更新不可通知がログイン認証装置300からファイアウォール200およびイントラネット100を介して所外端末10へ送信される（ステップS23、S14、S3）。

【0042】

しかし、ユーザIDがA003のユーザがウェブページA2の内容について変更または更新を行なう場合は、表1に示した認証テーブルのウェブページA2の欄に「●」印が記録してあるため、認証部301は照合後、ウェブページA2のアドレスおよびウェブページA2の内容の変更または更新を許可する情報をプロキシウェブサーバ400へ送信する（ステップS24）。

【0043】

ログイン認証装置300はプロキシウェブサーバ400へユーザのアクセス希望ウェブページのアドレス等を送信後、ユーザの当該ウェブページの利用回数を集計部303でカウントする（ステップS25）。カウントされた利用回数は、たとえば表1に示すように、認証テーブル上にて記録される。

【0044】

さらに集計部303は表2の認証テーブルを用いて、各工場コードや部コード、課コードごとのウェブページ利用回数を集計する（ステップS26）。集計結果を表2に示す。

【 0 0 4 5 】

【表 2】

		コンテンツ利用回数								
		サーバA			サーバB			サーバC		
		A1	A2	A3	B1	B2	B3	C1	C2	C3
工場コード	KUMA	100	250	23	55	78	95	12	62	91
	ITAMI	11	50	47
	FUKU

部コード	AXX	75	225	26	30	53	70	15	37	66
	BXX

課コード	100	15	165	5	0	28	10	0	2	6
	200

【 0 0 4 6 】

これにより、企業内の工場、部、または課ごとのウェブページ利用状況を容易に確認することが可能となり、利用状況に応じた各ウェブページの整理、内容の充実等を図ることが可能となる。

【 0 0 4 7 】

以上はユーザが所外端末 1 0 ～ N を用いた場合のログイン認証システムの動作を示したが、ユーザが拠点イ内の所内端末 1 ～ n を用いた場合についてもログイン認証システムは動作する。

【 0 0 4 8 】

図 3 はユーザが所内端末 1 を用いてウェブページにアクセスする場合のログイン認証システムの動作を示すフローチャート図である。

【 0 0 4 9 】

図 3 を参照して、ユーザが所内端末 1 を用いて、拠点イ内のウェブサーバ A 内のウェブページ A 2 にアクセスしたい場合、ユーザは所内端末 1 にユーザ ID およびパスワードおよびアクセスしたいウェブページ A 2 のアドレスをキーボードやマウス等の入力部（図示せず）により入力後、ログイン認証装置 3 0 0 に送信する（ステップ S 1）。

【 0 0 5 0 】

ログイン認証装置 3 0 0 は、所内端末 1 から送信されたユーザ ID およびパス

ワード、ウェブページA 2 のアドレスを受信後（ステップS 2 1）、受信したユーザIDおよびパスワードが認証テーブル上のユーザIDおよびパスワードと一致しているか否かを認証部3 0 1で確認し、さらにユーザがアクセスを希望するウェブページA 2について、ユーザがアクセス可能か否かを認証部3 0 1で認証する（ステップS 2 2）。なお認証は表1に示したマスタファイル3 0 2に記憶している認証テーブルを用いて行われる。

【0 0 5 1】

認証部3 0 1による認証方法については、図2に示したログイン認証システムの動作と同様であるので、説明は繰返さない。

【0 0 5 2】

認証の結果、認証部3 0 1が所内端末1からウェブページA 2へのアクセスを許可できないと判断した場合は、ログイン認証装置3 0 0から閲覧不可通知を直接所内端末1へ送信し（ステップS 2 3）、所内端末1にて閲覧通知不可通知を受信する（ステップS 2）

認証の結果、認証部3 0 1が所内端末1からウェブページA 2へのアクセスを許可できる場合の動作については、図2におけるステップS 2 4以降の動作と同様であるため、その説明は繰返さない。

【0 0 5 3】

以上のようにこの実施の形態によれば、ログイン認証装置3 0 0の設置により、ウェブページ単位でセキュリティの確保が可能となる。また、ユーザは各ウェブサーバ、各ウェブページへアクセスするたびにユーザIDとパスワードを入力するといった煩雑な操作から解放される。

【0 0 5 4】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと解釈されるべきである。本発明の範囲は上述した実施の形態ではなく特許請求の範囲によって定められ、特許請求の範囲と均等の意味およびその範囲内でのすべての変更が含まれることを意図するものである。

【0 0 5 5】

【発明の効果】

本発明によれば、ログイン認証装置 3 0 0 のマスタファイル 3 0 2 に認証テーブルを作成し、認証テーブル上で各ユーザが閲覧や更新のできるウェブページを管理しておくことで、イントラネット内のウェブサーバにおいて、ウェブページ単位でセキュリティを補償し、かつユーザにとって操作が単純であるログイン認証装置およびログイン認証方法を提供することができる。

【図面の簡単な説明】

【図 1】 この発明の実施の形態であるログイン認証システムの全体構成を示すブロック図である。

【図 2】 ユーザが所外端末 1 0 を用いてウェブページにアクセスする場合のログイン認証システムの動作を示すフローチャート図である。

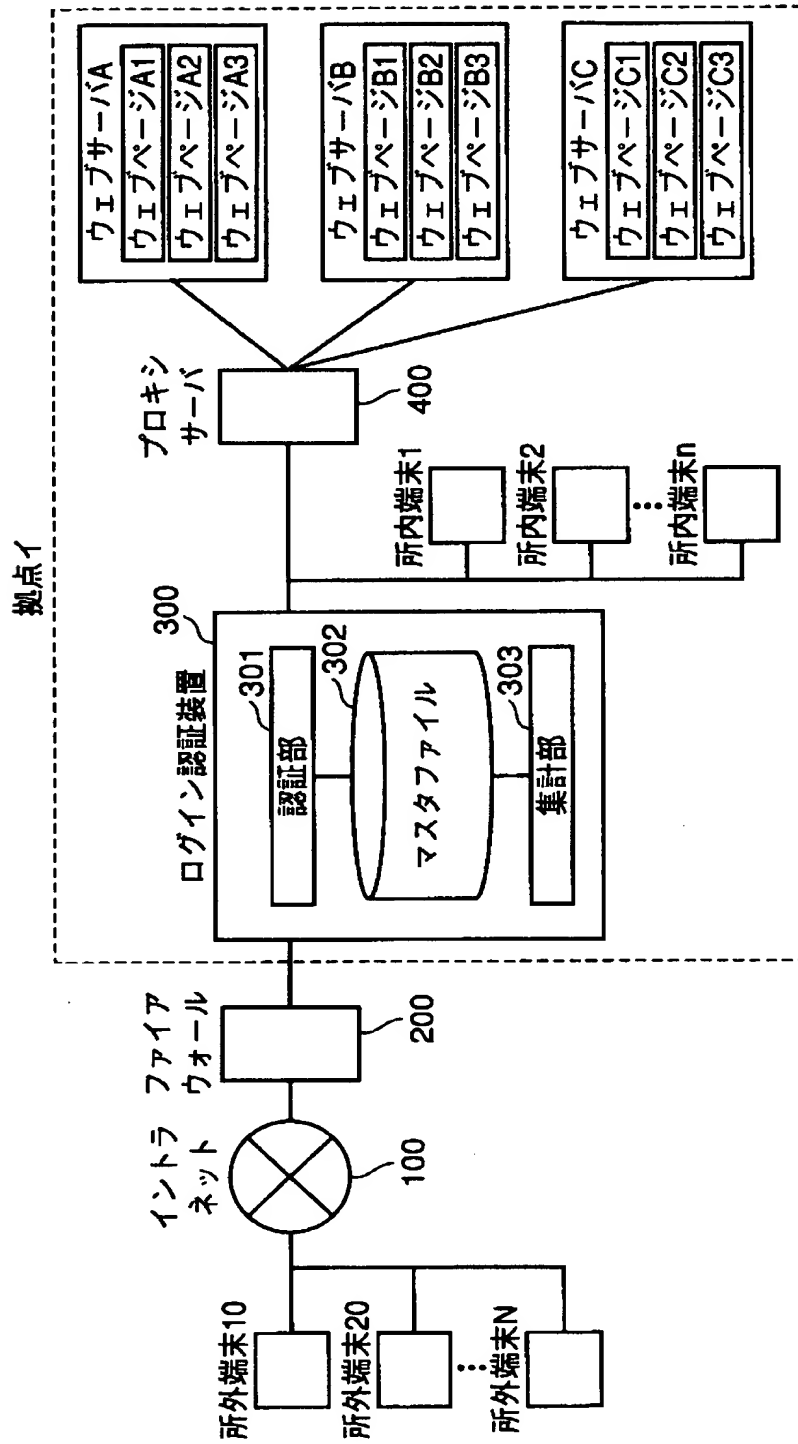
【図 3】 ユーザが所内端末 1 を用いてウェブページにアクセスする場合のログイン認証システムの動作を示すフローチャート図である。

【符号の説明】

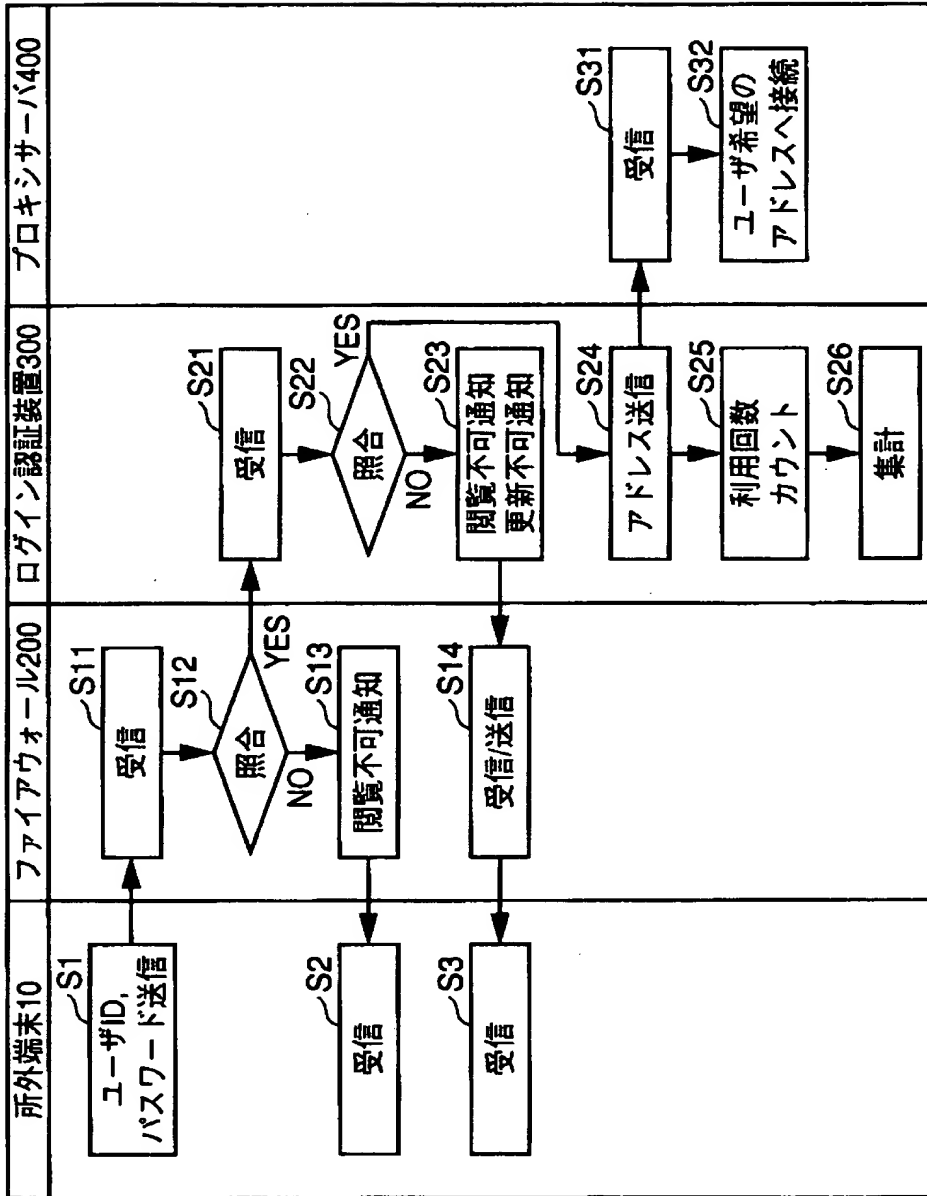
1 ～ n 所内端末、1 0 ～ N 所外端末、1 0 0 イン트라ネット、2 0 0 ファイアウォール、3 0 0 ログイン認証装置、3 0 1 認証部、3 0 2 マスタファイル、3 0 3 集計部、4 0 0 プロキシウェブサーバ。

【書類名】 図面

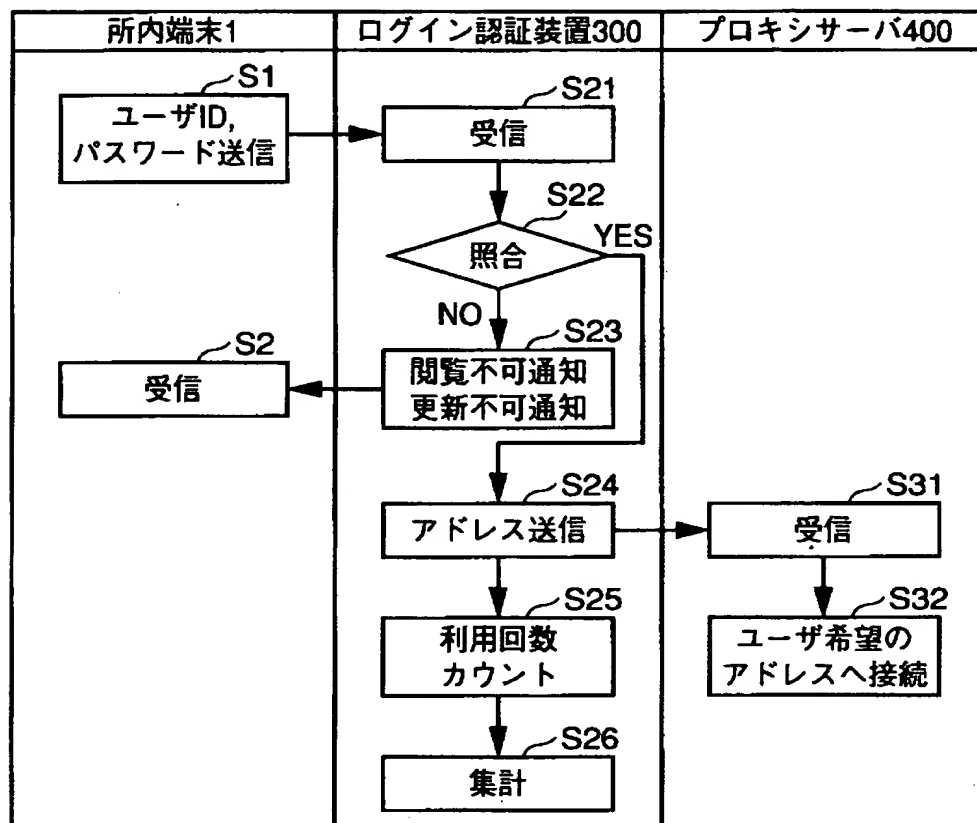
【図 1】



【図 2】



【図 3】



【書類名】 要約書

【要約】

【課題】 ウェブサーバ内のウェブページ単位でセキュリティを補償し、かつユーザにとって操作が簡単なログイン認証システムを提供する。

【解決手段】 所外端末 1 0 または所内端末 1 から送信されたユーザ I D と、パスワードと、ユーザがアクセスしたいウェブページのアドレスは、ログイン認証装置 3 0 0 にて受信され、マスタファイル 3 0 2 内の認証テーブル上のユーザ I D 等のデータと合致するか否かの認証が行われる。合致した場合は、ログイン認証装置 3 0 0 はウェブページのアドレスをプロキシサーバ 4 0 0 に送信し、その結果、ユーザはウェブページにアクセスすることができる。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000006013]

1. 変更年月日	1990年 8月24日
[変更理由]	新規登録
住 所	東京都千代田区丸の内2丁目2番3号
氏 名	三菱電機株式会社